Veterans Privacy Breach

Veterans' Administration's Data Breach

In an egregious breach of privacy, the personal and sensitive data of 26.5 million veterans, active-duty service members, members of the National Guard and Reserve personnel was stolen from the home of a Veteran's Administration official. Americans on active-duty, many overseas in Iraq and Afghanistan, are now distracted with the threat of identity theft back home. The Administration has clearly failed in its duty to protect those who have protected us. No other group of Americans has stood stronger and braver for our democracy than our men and women in uniform, and they deserve better.

House Democrats believe that the federal government has a duty to ensure that the financial health of our nation's veterans and military families is not harmed as a result of the VA's failure. To that end, we have called for an immediate investigation and review of the VA's security practices and how this breach happened, as well as introduced legislation protecting veterans and service members from identity theft and other harm. Veterans can visit http://www.firstgov.gov/ as well as www.va.gov/opa and www.ftc.gov/veterans for more information. In addition, the VA has set up a manned call center that veterans may call to get information about this situation and learn more about consumer identity protections: 1-800-FED INFO (333-4636), from 8 am to 9 pm (EDT), Monday-Saturday.

In response, Rep. Slaughter has sponsored H.R. 5455, the Veterans Identify Protection Act. It would require the Department of Veterans Affairs to provide veterans a year's worth of credit monitoring free of charge in addition to a free credit report in the next two years.

If you think that your personal and private data was stolen, take the following steps below to prevent identity theft:

Inspect your financial statements and monitor your financial accounts and billing statements to detect suspicious activity. Review financial accounts and billing statements regularly, looking for charges you did not make. Be alert to signs that require immediate attention:

- Bills that do not arrive as expected

- Unexpected credit cards or account statements

- Denials of credit for no apparent reason

- Calls or letters about purchases you did not make

Consider placing a "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting companies have toll-free numbers for placing an initial fraud alert; a call to one company should be sufficient for all three, but clarify that when you call:

- Equifax: 1-800-525-6285; http://www.equifax.com/; P.O. Box 740241, Atlanta, GA 30374-0241

- Experian: 1-888-EXPERIAN (397-3742); http://www.experian.com/; P.O. Box 2002, Allen, TX 75013

- TransUnion: 1-800-680-7289; http://www.transunion.com/; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

An initial fraud alert stays on your credit report for 90 days. When reviewing your credit reports, look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Placing a fraud alert also entitles you to additional free copies of your credit reports. Remember that you may find it more difficult to get new credit while there is a fraud alert on your credit file. You may want to check back after 90 days to reinstate your fraud alert.

>> Special Fraud Alert for Active Duty Military. If you are away from your permanent duty station, you may place a

special "active duty" fraud alert on your credit file to help minimize the risk of identity theft while you are deployed. Active duty alerts are in effect for one year, not just 90 days. If your deployment lasts longer than one year, you can place another alert on your credit file. You may place an active duty alert on your credit file by contacting any one of the nationwide consumer reporting companies mentioned above. You may use a personal representative to place or remove an alert. When you place an active duty alert, you'll be removed from the credit reporting companies' marketing list for pre-screened credit card offers for two years unless you ask to go back on the list before then.

Get your free credit reports. Credit reports contain information about you, including what accounts you have and your bill paying history. The law requires the major nationwide consumer reporting companies to give you a free copy of your credit report each year if you ask for it. Visit http://www.annualcreditreport.com/ or call 1-877-322-8228, a service created by these three companies, to order your free credit reports each year. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. To see changes over time, you may want to space your free requests out over the course of the year. (For example, request your Experian report now, your TransUnion report in four months and your Equifax report four months after that). You can ask the bureaus to send your credit report to you with only the last 4 digits of your Social Security number on it.

You may want to consider putting a "Security Freeze" on your credit reports. Some states allow consumers to "freeze" their credit file - limiting the ability of credit grantors to use the file in credit granting decisions. Some consumers choose not to freeze their accounts because it can be inconvenient to "unfreeze" the file if and when the consumer wants new credit, and there may be fees for unfreezing a file.

If you find suspicious activities:

- Immediately contact the credit bureau and the entity listed to have the information corrected (and fraudulent accounts closed)

- If a credit card/debit card was used, contact the issuer and alert them to the fraud/mistaken charges.

- Consider closing (or changing the account number) on any accounts that have been tampered with

- File a police report

- Report the theft to the Federal Trade Commission:

- Online: www.ftc.gov/idtheft

- By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261

- By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580